CLAIMS

What is claimed is:

1. A method comprising:

generating a list of update keys on a key distribution center system based on a table of secret keys identifying valid and invalid receivers of a plurality of receivers, said list of update keys allowing valid receivers to decrypt a valid content key using update keys obtained from the list of update keys;

generating a multiple nested list of decryption patterns based on the list of update keys;

broadcasting said multiple nested list of decryption patterns to the plurality of receivers;

recovering a content key from the list of update keys by recovering a set of update keys for each receiver from the multiple nested list of decryption patterns and using the set of update keys to decrypt the content key.

2. The method of claim 1, wherein said generating a list of update keys comprises generating at least one intermediate key and one content key.

3. The method of claim 2, wherein said generating at least one intermediate key and one content key comprises randomly generating said at least one intermediate key and one content key.

4. The method of claim 3, wherein authorized receivers will receive an intermediate key that allows recovery of a valid content key and unauthorized receivers will receive an intermediate key that does not allow recovery of a valid content key.

5. The method of claim 1, wherein said generating a multiple nested list of decryption patterns comprises encrypting an entry of the list of update keys using a key that is a combination of a previous update key, a secret key for a receiver associated with the entry of the list of update keys, and an index indicating a location in said table of secret keys associated with each entry.

6. The method of claim 5, wherein an entry in said multiple nested list of decryption patterns includes a predetermined test pattern encrypted with the secret keys for a receiver associated with the entry of the list of update keys.

7. The method of claim 1, wherein said recovering a set of update keys for each receiver from the multiple nested list of decryption patterns comprises parsing said multiple nested list of decryption patterns to locate an entry intended for a particular receiver based on detection of a predetermined test pattern included in an entry in the multiple nested list of decryption patterns.

8. The method of claim 1, further comprising broadcasting content encrypted with said content key.

9. The method of claim 8, further comprising decrypting said content encrypted with said content key using a content key recovered from the multiple nested list of decryption patterns.

10. A method comprising:

generating a list of update keys on a key distribution center system based on a table of secret keys identifying valid and invalid receivers of a plurality of receivers, said list of update keys allowing valid receivers to decrypt a valid content key using update keys obtained from the list of update keys;

generating a multiple nested list of decryption patterns based on the list of update keys; and

broadcasting said multiple nested list of decryption patterns to the plurality of receivers.

11. The method of claim 10, wherein said generating a list of update keys comprises generating at least one intermediate key and one content key.

12. The method of claim 11, wherein said generating at least one intermediate key and one content key comprises randomly generating said at least one intermediate key and one content key.

13. The method of claim 10, wherein said generating a multiple nested list of decryption patterns comprises encrypting an entry of the list of update keys using a key that is a combination of a previous update key, a secret key for a receiver associated with the entry of the list of update keys, and an index indicating a location in said table of secret keys associated with each entry.

14. The method of claim 13, wherein an entry in said multiple nested list of decryption patterns includes a predetermined test pattern encrypted with the secret keys for a receiver associated with the entry of the list of update keys.

15. A method comprising:

receiving a multiple nested list of decryption patterns from a key distribution center system;

recovering a set of update keys from the multiple nested list of decryption patterns; and

recovering a content key from the list of update keys by using the set of update keys to decrypt the content key.

16. The method of claim 15, wherein said multiple nested list of decryption patterns comprises a list of update keys encrypted with a key that is a combination of a previous update key, a secret key for a receiver associated with an entry of the list of update keys, and an index value.

17. The method of claim 16, wherein an entry in said multiple nested list of decryption patterns includes a predetermined test pattern encrypted with secret keys for a receiver associated with the entry of the list of update keys.

18. The method of claim 15, wherein said recovering a set of update keys from the multiple nested list of decryption patterns comprises parsing said multiple nested list of decryption patterns to locate an entry intended for a particular receiver based on detection of a

predetermined test pattern included in an entry in the multiple nested list of decryption patterns.

19. A system comprising:

a key distribution center to generate a list of update keys based on a table of secret keys identifying valid and invalid receivers of a plurality of receivers, said list of update keys allowing valid receivers of said plurality of receivers to decrypt a valid content key using update keys obtained from the list of update keys, generate a multiple nested list of decryption patterns based on the list of update keys, and broadcast said multiple nested list of decryption patterns to the plurality of receivers; and

a content receiver to recover an appropriate set of update keys from the multiple nested list of decryption patterns so that the final key recovered in the set of update keys is a content key.

20. The system of claim 19, wherein said key distribution center generates at least one intermediate key and one content key.

21. The system of claim 20, wherein said key distribution center randomly generates said at least one intermediate key and one content key.

22. The system of claim 21, wherein authorized receivers will receive an intermediate key that allows recovery of a valid content key and unauthorized receivers will receive an intermediate key that does not allow recovery of a valid content key.

23. The system of claim 19, wherein said key distribution center encrypts an entry of the list of update keys using a key that is a combination of a previous update key, a secret keys for a receiver associated with the entry of the list of update keys, and an index indicating a location in said table of secret keys associated with each entry to generate said multiple nested list of decryption patterns.

24. The system of claim 23, wherein an entry in said multiple nested list of decryption patterns includes a predetermined test pattern encrypted with the secret keys for a receiver associated with the entry of the list of update keys.

25. The system of claim 19, wherein said receiver parses said multiple nested list of decryption patterns to locate an entry intended for a particular receiver based on detection of a predetermined test pattern included in an entry in the multiple nested list of decryption patterns.

26. The system of claim 19, further comprising content provider to broadcast content encrypted with said content key.

27. The system of claim 26, wherein said receiver decrypts said content encrypted with said content key using a content key recovered from the multiple nested list of decryption patterns.

28. A machine-readable medium having stored thereon data representing sequences of instructions, the sequences of instructions which, when executed by a processor, cause the processor to:

generate a list of update keys on a key distribution center system based on a table of secret keys identifying valid and invalid receivers of a plurality of receivers, said list of update keys allowing valid receivers to decrypt a valid content key using update keys obtained from the list of update keys;

generate a multiple nested list of decryption patterns based on the list of update keys;

broadcast said multiple nested list of decryption patterns to the plurality of receivers;

recover a content key from the list of update keys by recovering an appropriate set of update keys for each receiver from the multiple nested list of decryption patterns and using the set of update keys to decrypt the content key.

29. The machine-readable medium of claim 28, wherein said generating a list of update keys comprises generating at least one intermediate key and one content key.

30. The machine-readable medium of claim 29, wherein said generating at least one intermediate key and one content key comprises randomly generating said at least one intermediate key and one content key.

31. The machine-readable medium of claim 30, wherein authorized receivers will receive an intermediate key that allows recovery of a valid content key and unauthorized receivers will receive an intermediate key that does not allow recovery of a valid content key.

32. The machine-readable medium of claim 28, wherein said generating a multiple nested list of decryption patterns comprises encrypting an entry of the list of update keys using a key that is a combination of a previous update key, a secret keys for a receiver associated with the entry of the list of update keys, and an index indicating a location in said table of secret keys associated with each entry.

33. The machine-readable medium of claim 32, wherein an entry in said multiple nested list of decryption patterns includes a predetermined test pattern encrypted with the secret keys for a receiver associated with the entry of the list of update keys.

34. The machine-readable medium of claim 28, wherein said recovering an appropriate set of update keys for each receiver from the multiple nested list of decryption patterns comprises parsing said multiple nested list of decryption patterns to locate an entry intended for a particular receiver based on detection of a predetermined test pattern included in an entry in the multiple nested list of decryption patterns.

35. The machine-readable medium of claim 28, further comprising broadcasting content encrypted with said content key.

36. The machine-readable medium of claim 35, further comprising decrypting said content encrypted with said content key using a content key recovered from the multiple nested list of decryption patterns.

37. A machine-readable medium having stored thereon data representing sequences of instructions, the sequences of instructions which, when executed by a processor, cause the processor to:

generate a list of update keys on a key distribution center system based on a table of secret keys identifying valid and invalid receivers of a plurality of receivers, said list of update keys allowing valid receivers to decrypt a valid content key using update keys obtained from the list of update keys;

generate a multiple nested list of decryption patterns based on the list of update keys; and

broadcast said multiple nested list of decryption patterns to the plurality of receivers.

38. The machine-readable medium of claim 37, wherein said generating a list of update keys comprises generating at least one intermediate key and one content key.

39. The machine-readable medium of claim 38, wherein said generating at least one intermediate key and one content key comprises randomly generating said at least one intermediate key and one content key.

40. The machine-readable medium of claim 37, wherein said generating a multiple nested list of decryption patterns comprises encrypting an entry of the list of update keys using a key that is a combination of a previous update key, a secret key for a receiver associated with the entry of the list of update keys, and an index indicating a location in said table of secret keys associated with each entry.

41. The machine-readable medium of claim 40, wherein an entry in said multiple nested list of decryption patterns includes a predetermined test pattern encrypted with the secret keys for a receiver associated with the entry of the list of update keys.

42. A machine-readable medium having stored thereon data representing sequences of instructions, the sequences of instructions which, when executed by a processor, cause the processor to:

receive a multiple nested list of decryption patterns from a key distribution center system;

recover a set of update keys from the multiple nested list of decryption patterns; and

recover a content key from the list of update keys by using the set of update keys to decrypt the content key.

43. The machine-readable medium of claim 42, wherein said multiple nested list of decryption patterns comprises a list of update keys encrypted with a key that is a combination of a previous update key, a secret key for a receiver associated with an entry of the list of update keys, and an index value.

44. The machine-readable medium of claim 43, wherein an entry in said multiple nested list of decryption patterns includes a predetermined test pattern encrypted with secret keys for a receiver associated with the entry of the list of update keys.

45. The machine-readable medium of claim 42, wherein said recovering a set of update keys from the multiple nested list of decryption patterns comprises parsing said multiple nested

list of decryption patterns to locate an entry intended for a particular receiver based on detection of a predetermined test pattern included in an entry in the multiple nested list of decryption patterns.